

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

Nina McClain, <i>on behalf of herself and all others similarly situated,</i> Plaintiff, v. HENRY FORD HEALTH, Defendant.	Case No. _____ CLASS ACTION COMPLAINT JURY TRIAL DEMANDED
-----------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------

CLASS ACTION COMPLAINT

1. Plaintiff Nina McClain, at all times relevant herein, has been a patient of Henry Ford Health (“Henry Ford” or “Defendant”), and brings this class action against Defendant in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, her counsels’ investigation, and upon information and belief as to all other matters, as follows:

2. Plaintiff brings this case to address Defendant’s unlawful practice of disclosing Plaintiff’s and Class Members’ confidential personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “Private Information”) to third parties, including Meta Platforms, Inc. d/b/a

Meta (“Facebook”) and Google, Inc. (“Google”), without consent, through the use of tracking software that is embedded in Defendant’s website.

3. Defendant owns and controls <https://www.henryford.com/> (“Defendant’s Website” or the “Website”), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, and more.

4. Included within Defendant’s Website is the MyChart Patient Portal (<https://mychart.HenryFords.org/mychart/Authentication/Login>), which Defendant encourages patients to sign up for and use so that they can more conveniently book appointments and schedule visits, review their health records and test results, pay bills, communicate with service providers, request prescription refills, and complete medical forms virtually and remotely.

5. Unbeknownst to patients, starting as early as June 2015 Defendant installed third-party tracking technologies such as the Facebook Pixel and Google Analytics, Google Tag Manager, and Google DoubleClickAds (“Tracking Tools”) onto its Website, including, upon information and good faith belief, the Patient Portal.¹ These Tracking Tools, such as pixels, web beacons, tags, or cookies, track

¹ MyChart is run by a third party, Epic Software Systems (Epic), which permits its

and collect communications with the Defendant via the Website and surreptitiously force the user's web browser to send those communications to undisclosed third parties, such as Facebook or Google.²

6. Plaintiff and Class Members used the Website to submit information related to their past, present, or future health conditions, including, for example, searches for specific health conditions and treatment and the booking of specialized classes or medical appointments with specific physician. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care from Defendant, as well as the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or addiction.

7. Facebook connects user data from Defendant's Website to the individual's Facebook ID (FID). The FID links the user to her/his Facebook profile,

partners to deploy "custom analytics scripts." Tracking technologies can be embedded into the code, and because of Defendant's pervasive use of tracking technologies on its Website, including its MyChart landing page, upon information and belief Plaintiff avers that tracking technologies were also deployed in the MyChart Portal.

² While this Complaint focuses on tracking codes from Facebook and Google, Plaintiff's counsel's investigation shows that Henry Ford also installed trackers from CallRail, CrazyEgg, HotJar, Centro/SiteScout Basis, LinkedIn, Pinterest Business, and SkyGlue.

which contains detailed information about the profile owner’s identity sufficient to identify them personally.

8. Similarly, Google “stores users’ logged-in identifier on non-Google websites...in its logs ... Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user’s browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads.”³

9. Facebook tracks and collects data even on people who do not have a Facebook account or have deactivated their Facebook accounts. Those individuals can find themselves in an even worse situation because even though their Private Information is sent to Facebook—without their consent—they cannot clear past

³ See *Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023) (order denying summary judgment and citing internal evidence from Google employees). Google also connects user data to IP addresses. IP addresses have been classified by the United States Department of Health and Human Services (“HHS”) as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html> (“Such PHI may include, for example, an individual’s IP address . . .”) (last visited June 16, 2024).

activity or disconnect the collection of future activity since they do not possess an account (or an active account).⁴

10. Then, completely unencumbered by any pretense of restriction or regulation, Facebook and Google, in turn, use that Private Information for various business purposes, including using such information to “improve” advertisers’ ability to target specific demographics and selling such information to third-party marketers who target those Users online (through their Facebook, Instagram, Gmail and other social media and personal accounts):

Along with encouraging businesses to spend ad dollars, Facebook also receives the transmitted data, and can use it to hone its algorithms. Facebook can also use data from the pixel to link website visitors to their Facebook accounts, meaning businesses can reach the exact people who visited their sites. The pixel collects data regardless of whether the visitor has an account.⁵

⁴ In the past, these were referenced as “ghost accounts” or “shadow profiles.” See Laura Hautula, *Shadow profiles: Facebook has information you didn’t hand over*, CNET (April 11, 2018), <https://www.cnet.com/news/privacy/shadow-profiles-facebook-has-information-you-didnt-hand-over/>.

⁵ See Colin Lecher & Ross Teixeira, *Facebook Watches Teens Online As They Prep For College*, THE MARKUP (Nov. 22, 2023), <https://themarkup.org/pixel-hunt/2023/11/22/facebook-watches-teens-online-as-they-prep-for-college#:~:text=After%20signing%20into%20their%20ACT,re%20registering%20for%20the%20ACT> (stating that “[b]usinesses embed the pixel on their own websites voluntarily, to gather enough information on their customers so they can advertise to them later on Meta’s social platforms”) (last visited June 14, 2024)..

11. Simply put, the health information disclosed through the tracking technologies is personally identifiable.

12. In addition to the Tracking Tools, upon information and belief Defendant also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Website servers.⁶

13. Unlike the Facebook Pixel which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.^{7, 8} Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution

⁶ "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." See <https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited Mar. 15, 2024).

⁷ <https://revealbot.com/blog/facebook-conversions-api/> (last visited June 15, 2024).

⁸ "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel.... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited June 15, 2024).

across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results.”⁹

14. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly

15. Defendant utilized the Pixel and CAPI data for marketing purposes to bolster its profits. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data and information from users' communications with the Website to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

16. The information disclosed in this way by Defendant allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to

⁹<https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited June 15, 2024).

third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI.

17. Defendant is a healthcare entity and thus its disclosure of health and medical communications is tightly regulated. The United States Department of Health and Human Services (HHS) has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

18. In addition, as explained further below, HHS has specifically warned healthcare regulated entities that tracking technologies like those used by Defendant transmit personally identifying information to third parties, both on the public portion of the website and within the password-protection patient portal, and that such information should not be transmitted without a HIPAA-acceptable written authorization from patients.

19. The Federal Trade Commission (FTC) has also warned hospitals and other entities that "even if you are not covered by HIPAA, you still have an

obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule.”

20. The Michigan Nonprofit Health Care Corporation Reform Act states that healthcare entities are required to provide reasonable care in securing their members’ healthcare records from unauthorized access and to collect only personal data that is necessary for payment of claims, treatment and research. It further states that the healthcare entity cannot disclose any records containing personal data of any member without written notice and written consent of that member. MCL 550.1406.

21. Further, the Michigan Public Health Code states that a “patient or resident is entitled to confidential treatment of personal and medical records, and may refuse their release to a person outside the health facility or agency except as required because of a transfer to another health care facility, as required by law or third party payment contract, or as permitted or required under the health insurance portability and accountability act of 1996, Public Law 104-191, or regulations promulgated under that act, 45 CFR parts 160 and 164.” MCL 333.20201(2)(c).

22. Despite these warnings, Defendant has embedded hidden Tracking Tools and CAPI on its Website and servers, essentially planting a bug on patients’ web browsers that forced them disclose private and confidential communications to third parties. Defendant did not disclose the presence of these Tracking Tools to its patients and Website users.

23. Healthcare patients simply do not anticipate or expect that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party – let alone Facebook and Google, which both have a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients’ consent. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook or Google.

24. Defendant breached its statutory and common law obligations to Plaintiff and Class Members by, inter alia: (i) failing to remove or disengage technology that was known and designed to share web-users’ information; (ii) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook, Google or others; (iii) failing to take steps to block the transmission of Plaintiff’s and Class Members’ Private Information through Tracking Tools like the Facebook Pixel, Google Analytics or CAPI; (iv) failing to warn Plaintiff and Class Members; and (v) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

25. As a result of Defendant’s conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of

the bargain, (iii) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk to their Private Information.

26. Plaintiff seeks to remedy these harms and brings causes of action for (1) breach of fiduciary duty/confidentiality; (2) violation of the Electronics Communication Privacy Act (“ECPA”) 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (3) invasion of privacy; (4) breach of implied contract; (5) unjust enrichment; (6) negligence; and (7) violation of the Michigan Nonprofit Health Care Corporation Reform Act, MCL § 550.1406.

PARTIES

27. Plaintiff Nina McClain is a natural person and citizen of Michigan where she intends to remain.

28. Defendant Henry Ford Health is a Michigan-based Health Care Provider with its principal place of business located at One Ford Place, Suite 5B, Detroit, Michigan 48202.

29. Defendant serves a growing number of customers across more than 250 locations throughout Michigan including five acute care hospitals, two destination facilities for complex cancer and orthopedics and sports medicine care, three behavioral health facilities, primary care, and urgent care centers.¹⁰

¹⁰ <https://www.henryford.com/about> (last visited June 20, 2024).

30. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 (HIPAA)).

JURISDICTION & VENUE

31. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

32. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges one or more question(s) of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*).

33. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

34. Venue is proper under 28 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

A. Federal Regulators Make Clear that the Use of Tracking Technologies to Collect & Divulge Private Information Without Informed Consent is Illegal

35. This surreptitious collection and divulgence of Private Information is an extremely serious data security and privacy issue. Both the Federal Trade Commission and the Office for Civil Rights (“OCR”) of the Department of Health and Human Services (“HHS”) have, in recent months, reiterated the importance of and necessity for data security and privacy concerning health information.

36. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker’s dozen takeaways from FTC cases*, in which it noted that “[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer’s health.*** Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning ‘pregnancy mode’ on or off) may itself be health information.***”¹¹

37. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to

¹¹ See Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, FTC Business Blog (July 25, 2023) (emphasis added), <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases>.

collect sensitive health information and disclose it to various platforms without informed consent:

Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.

In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. *But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.*

[Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that *may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information.*¹²

38. The federal government is taking these violations of health data privacy and security seriously as recent high-profile FTC settlements against several telehealth companies' evidence. For example, earlier this year, the FTC imposed a \$1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and platforms, including Facebook,

¹² *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

Google and Criteo, and a \$7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Facebook and Snapchat for advertising purposes. And Easy Healthcare was ordered to pay a \$100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app Premon shared health data for advertising purposes.¹³

39. Even more recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about using online tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the “risks and concerns about the use of technologies, such as the Meta/Facebook Pixel and Google Analytics, that can track

¹³ See *How FTC Enforcement Actions Will Impact Telehealth Data Privacy*, Health IT Security, <https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy> (last visited June 14, 2024); See Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), www.law360.com/articles/1571369/ftc-targets-goodrx-in-1st-action-under-health-breach-rule?copied=1 (“The Federal Trade Commission signaled it won’t hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale.”); <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising>; <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premon-will-be-barred-sharing-health-data-advertising-under-proposed-ftc> (last visited June 14, 2024).

a user’s online activities,” and warned about “[i]mpermissible disclosures of an individual’s personal health information to third parties” that could “result in a wide range of harms to an individual or others.” According to the letter, “[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more.”¹⁴

¹⁴ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, Dept. of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.htm> (noting that “IIHI collected on a regulated entity’s website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.”). This guidance was recently vacated *in part* by the Federal District Court for the Northern District of Texas due to the court finding it in part to be the product of improper rulemaking and it is cited for reference only until the OCR updates its guidance, should it do so in the future. See *American Hosp. Ass’n. v. Becerra*, No. 4:23-cv-01110-P, ECF No. 67 (S.D. Tex., Jun. 20, 2024). Notably, the court’s order found only that the OCR’s guidance regarding covered entities disclosing to third parties users’ IP addresses while users navigated *unauthenticated public webpages* (“UPWs”) was improper rulemaking. The Order in no way affects or undermines the OCR’s guidance regarding covered entities disclosing personal identifiers, such as Google or Facebook identifiers, to third parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. See *id.* at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the “Proscribed Combination” defined as “circumstances where an online technology connects (1) an individual’s IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers” but stating that “[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document.”). Furthermore, the FTC bulletin on the same topics

40. Moreover, the Office for Civil Rights at HHS has made clear, in a recent bulletin titled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA's Privacy Rule:

Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.¹⁵

41. The OCR Bulletin discusses the harms that disclosure may cause patients:

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, *discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.* Such disclosures can reveal incredibly sensitive information about an individual, *including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.* While it has always been true that regulated

remains untouched, as do the FTC's enforcement actions against healthcare providers for committing the same actions alleged herein).

¹⁵ *Id.*

entities may not impermissibly disclose PHI to tracking technology vendors, *because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*¹⁶

42. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to monetize their Users' Private Information.

43. For instance, THE MARKUP reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.¹⁷

44. And, in the aptly titled report "*Out of Control*": *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and THE MARKUP of 50 direct-to-consumer telehealth companies reported that telehealth companies or virtual care websites were

¹⁶ *Id.* (emphasis added).

¹⁷ See Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.

providing sensitive medical information they collect to the world's largest advertising platforms.¹⁸

Many telehealth sites had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn and/or Pinterest—that collected patients' answers to medical intake questions.¹⁹

B. Underlying Web Technology

45. To understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and tracking tools.

46. Devices (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

47. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

¹⁸ Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools*, The Markup (Dec. 13, 2022), <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>.

¹⁹ *See id.* (noting that "[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan").

48. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **Universal Resource Locator (“URL”):** a web address.
- **HTTP Request:** an electronic communication sent from the client device’s browser to the website’s server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL, GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies:** a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are “third-party cookies,” which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response:** an electronic communication that is sent as a reply to the client device’s web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.²⁰

49. A patient’s HTTP Request essentially asks the Defendant’s Website to retrieve certain information (such as “Find a Doctor” page). The HTTP Response sends the requested information in the form of “Markup.” This is the foundation for the pages, images, words, buttons, and other features that appear on the patient’s screen as they navigate Defendant’s Website

²⁰ One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

50. Every website is comprised of Markup and “Source code.” Source code is simply a set of instructions that commands the website visitor’s browser to take certain actions when the web page first loads or when a specified event triggers the code. Source code is essentially the back of the website, and the user does not see what happens in the source code.

51. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser’s user. Defendant’s implementation of the Tracking Tools is source code that does just that. The Tracking Tools act much like a traditional wiretap. When patients visit Defendant’s Website via an HTTP Request to Henry Ford Health’s server, the server sends an HTTP Response including the Markup that displays the webpage visible to the user and Source Code including the Tracking Tools. Thus, Defendant is in essence handing patients a tapped phone, and once the webpage is loaded into the patient’s browser, the software-based wiretap is quietly waiting for private communications on the Website to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third parties, including Facebook and Google.

52. Third parties, like Facebook and Google, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify

the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Private Information intercepted.

53. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that savvy users cannot evade. Facebook’s workaround, for example, is CAPI. CAPI is an effective workaround because transmits information from Defendant’s own servers and does not rely on the user’s web browsers. CAPI “is designed to create a direct connection between [Website hosts’] marketing data and [Facebook].” Thus, the communications between patients and Defendant, which are necessary to use Defendant’s Website, are received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

54. While there is no way to confirm with certainty that a Website host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to “[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools,” because such a “redundant event setup” allows Defendant “to share website events [with

Facebook] that the pixel may lose.”²¹ Thus, it is reasonable to infer that Facebook’s customers who implement the Facebook Pixel in accordance with Facebook’s documentation will also implement the CAPI workaround.

55. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive Website content relating to the user’s communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (i.e., to bolster profits).

56. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user’s computing device, causing the device to contemporaneously and invisibly re-direct the user’s communications to third parties.

57. In this case, Defendant employed the Tracking Tools and CAPI to intercept, duplicate, and re-direct Plaintiff’s and Class Members’ Private Information to Facebook.

58. By contrast, the Markup is the façade of the Website and what the user sees.

²¹ *See*

<https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last visited Mar. 15, 2024).

59. As an example, a patient's HTTP Request seeks specific information from the Defendant's Website (e.g., "Find a Doctor" page), and the HTTP Response provides the requested information in the form of "Markup," forming the webpage's content and features.

60. As the example below illustrates, when a patient visit <https://www.henryford.com> and selects the "Doctors" button, the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that webpage. As depicted below, the user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

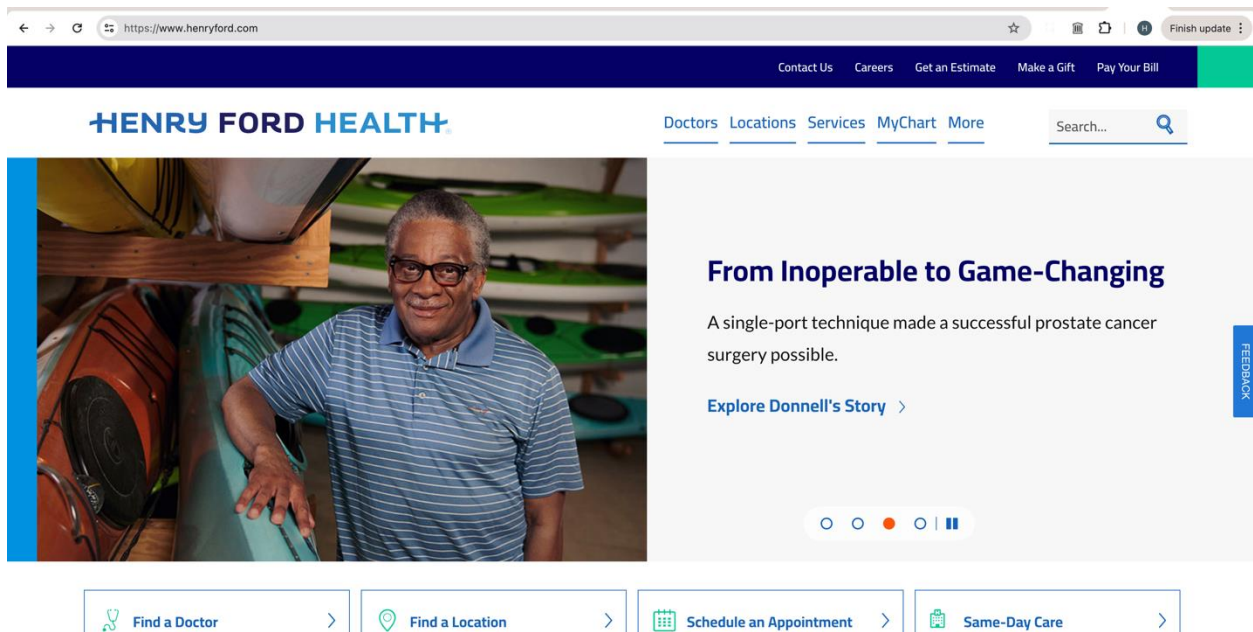


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting <https://www.henryford.com/> (last accessed Jun. 17, 2024).

61. The image above displays the Markup of Defendant's Webpage. Behind the scenes and in the backdoor of the webpage, tracking technologies like the Facebook Pixel and the Google Analytics tracking tool are embedded in the Source code, automatically transmitting what the patient does on the webpage and effectively opening a hidden spying window into the patient's browser.²²

C. Tracking Tools

62. Third parties, like Facebook and Google, offer Tracking Tools as free software that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user communications and activity on those platforms. The Tracking Tools are used to gather, identify, target, and market products and services to individuals.

63. In general, Tracking Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's URL and metadata, button clicks, etc. Advertisers, such as Defendant, can track other user actions and communications and can create their own tracking parameters by customizing the software on their website.

²² When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. For example, the Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

64. When a user accesses a webpage that is hosting Tracking Tools, the user's communications with the host webpage are instantaneously and surreptitiously duplicated and sent to the third party. For example, the Facebook Pixel on Defendant's Website causes the user's web browser to instantaneously duplicate the contents of the communication with the Website and send the duplicate from the user's browser directly to Facebook's server.

65. Google Analytics tracking tool is marginally different than the Facebook Pixel, but essentially accomplishes the same goal; tracking what a user communicates to Defendant's website.²³

66. Notably, transmissions only occur on webpages that contain Tracking Tools.²⁴ Thus, Plaintiff's and Class Member's Private Information would not have

²³ *Comparing Google Analytics vs Facebook Pixel*, Boltic, <https://www.boltic.io/blog/google-analytics-vsfacebookpixel#:~:text=Google%20Analytics%20is%20a%20comprehensive,time%20on%20site%2C%20and%20conversions.&text=On%20the%20other%20hand%2C%20Facebook,user%20actions%20on%20your%20website>. (last visited June 20, 2024)

²⁴ Defendant installed several Facebook Pixels during the relevant period, each of which has its own unique identifier (including Pixels with id=1545396389050955, id=367464206935045, id=1025144617598163, id=473478176677100 and id=667196134406461), which can be used to identify which of Defendant's webpages contain the Facebook Pixel. Similarly, Defendant's Google Tracking Tools have unique identifying numbers of their own, such as its GTM container with ID GTM-N9HBCDH.

been disclosed to Facebook or Google via this technology but for Defendant's decisions to install the Tracking Tools on its Website.

67. Sometimes a particularly tech-savvy user attempts to circumvent browser-based wiretap technology, so a website operator can also transmit data directly to Facebook using first-party cookies (CAPI server-to-server transmission). Users cannot detect or prevent transmissions through first-party cookies.

68. CAPI is another Facebook tool that functions as a redundant measure to circumvent any ad blockers or other denials of consent by the website user by transmitting information directly from Defendant's servers to Facebook's servers.²⁵ ²⁶ Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."²⁷

²⁵*What is the Facebook Conversions API and how to use it*, Realbot (last updated May 20, 2022), <https://revealbot.com/blog/facebook-conversions-api/> (last visited June 20, 2024).

²⁶ "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel.... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." See <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited June 20, 2024).

²⁷*About Conversions API*, Meta Business Help Center, <https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited June 20, 2024).

69. The third parties to whom a website transmits data through Tracking Tools and associated workarounds (CAPI) do not provide any substantive Website content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (*i.e.*, to bolster profits).

70. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

D. Defendant Disclosed Plaintiff's and Class Members' Private Information to Facebook and Google Using Tracking Tools

71. In this case, Defendant employed Tracking Tools, including the Facebook Pixel and Conversions API, as well as the Google Analytics tool, to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook and Google.

72. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook and Google. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

73. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" its patients' computing devices, allowing Facebook, Google, and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

74. The Tracking Tools allow Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs. However, Defendant's Website does not rely on the Tracking Tools in order to function.

75. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

76. Plaintiff and Class Members were not aware that their Private Information would be shared with third parties as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

77. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to third parties, nor did they intend for anyone other than Defendant to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

78. Defendant's Tracking Tools sent non-public Private Information to third parties like Facebook and Google, including but not limited to Plaintiff's and Class Members': (1) status as medical patients including their prescription, bill pay, medical record requests, and MyChart activities; (2) health conditions; (3) desired medical treatment or therapies; (4) desired locations or facilities where treatment was sought; (5) phrases and search queries (such as searches for symptoms, treatment options, or types of providers); (6) searched and selected physicians and their specialties conducted via the Website search bar; (7) appointment scheduling activities and (8) details of their registration for specific healthcare-related medical classes.

79. Importantly, the Private Information Defendant's Tracking Tools sent to third parties included personally identifying information that allowed those third parties to connect the Private Information to a specific patient. Information sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.²⁸

²⁸ Defendant's Website tracks and transmits data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent

80. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including location, pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

81. Similar to Facebook, the Private Information Defendant's Tracking Tools sent to third parties included personally identifying information that allowed those third parties to connect the Private Information to a specific patient. Information sent to Google was sent alongside the Plaintiff's and Class Members' unique identifier (“_ga” or “CID”) , thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Google accounts and therefore their identity.²⁹

set of numbers that can be easily used to look up that person's Facebook account by simply typing the numbers after www.facebook.com/ and hitting “Enter.”.

²⁹ See *Brown v. Google LLC*, 2023 WL 5029899, at fn. 11, *supra*, note 3 (quoting Google employee deposition testimony explaining how Google tracks user data).

82. Google logs a user's browsing activities on non-Google websites and uses these data for serving personalized ads.

83. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented Tracking Tools that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to unauthorized third parties; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

84. By installing and implementing both Facebook tools and Google Analytics, Defendant caused Plaintiff's and Class Member's communications to be intercepted by and/or disclosed to Facebook and Google and for those communications to be personally identifiable.

85. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

E. Defendant's Tracking Tools Disseminate Patient Information Via Its Website

86. An example illustrates the point. If a patient uses the Website to find a Doctor, Defendant's Website directs them to communicate Private Information, including the particular doctor, specialty, or conditions the patient has or is seeking.

Unbeknownst to the patient, each and every communication is sent to third parties, namely Facebook and Google, via Defendant's Tracking Tools, including the physician the patient selects, the location of that physician, and any text or phrases the patient types into the search bar.

87. In the example below, the user navigated to the "Doctors" page in Defendant's Website:

The screenshot shows the Henry Ford Health website's physician directory search results. On the left, a 'Filter Your Search' sidebar contains various filters: 'Schedule Online' (checkbox), 'Accepting New Patients' (checkbox), 'Specialties, Services and Conditions' (dropdown set to 'Cancer'), 'Provider's Name' (text input), 'Henry Ford Medical Group' (checkbox), 'Zip Code' (text input with a 'Use my current location' link), 'Location Name' (dropdown), 'Admitting Hospital' (dropdown), 'Language' (dropdown), and 'Gender' (dropdown). A green 'Search' button is at the bottom of the filters. The main content area is titled 'Find a Doctor or Provider Search Results' and shows '175 results'. Three doctor profiles are displayed: 1. Firas F Abdollah, MD, Urology, Henry Ford Medical Center - Lakeside. 2. Muwaffak M Abdulhak, MD, Neurological Surgery, Henry Ford Hospital K Building. 3. Marwan S Abouljoud, MD. Each profile includes a photo, name, contact info, specialties, services, and location. The Henry Ford logo is visible in the top right of the search results area.

Figure 2. Screenshot taken from <https://www.henryford.com/physician-directory> as the user searches for a specialist in cancer and communicates information via the search bar and filtering tools.

88. Next, the user was prompted to filter the results by, among other categories, the provider's specialty and location, ability to schedule an appointment online, whether they accept new patients, language, and gender.

89. Unbeknownst to ordinary patients, this webpage showing user's search results—which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Defendant's Tracking Tools. The image below shows the “behind the scenes” portion of the website that is invisible to ordinary users. Importantly, each entry in the column represents just one instance in which Defendant's Tracking Tools sent this user's information to Facebook:

The screenshot shows a web browser with two tabs: "Search Result | Henry Ford Health" and "Accounts Center". The address bar shows the URL: `henryford.com/physician-directory/search-results?#scheduleonline=&Medical%20Group=&AcceptsNewPatients=&physicianspecialties=Oncology&providersname=&o=PhysicianName&...`. The page displays the Henry Ford Health logo and a search filter section titled "Filter Your Search". Below this is a section titled "Find a Doctor or Provider Search Results" showing 93 results. A profile for Muneeb M Abidi, MD, is visible, including a photo, contact information (800-436-7936), specialties (Hematology), services (Hematology & Oncology, Medical Oncology, Stem Cell Transplant, Video Visits), and address (Henry Ford Cancer - Detroit, 2800 W Grand Blvd, Detroit, MI 48202). The browser's developer tools are open, showing the "Network" tab with a list of requests. A red box highlights a request to "facebook" with a "Query String Parameters" section. The parameters include: `id: 367464206935045`, `ev: PageView`, `dl: https://www.henryford.com/physician-directory/search-results?#scheduleonline=&Medical%20Group=&AcceptsNewPatients=&physicianspecialties=Oncology&providersname=&o=PhysicianName&...`, and `rl: https://www.henryford.com/physician-directory`. Other parameters like `if: false`, `ts: 1715461853381`, `sw: 5120`, `sh: 1440`, `v: 2.9.57`, `r: stable`, `ec: 0`, `o: 30`, `fbpr: fb.1.1713898718168.987348109`, `it: 1715461852863`, `coo: false`, and `rqm: GET` are also visible.

Figure 3. Screenshot showing the Markup (user-facing portion of the website) alongside the network traffic which discloses the details of the user's search result for an oncologist. Each entry in the column to the right represents one instance in which the user's information was transmitted to Facebook via Defendant's pixel.

90. Thus, without alerting the user, Defendant's Tracking Tools sent each and every communication the user made via the webpage to Facebook, and the images below confirm that the communications Defendant sent to Facebook contain the user's Private Information.

91. The following images reveal what information is sent to Facebook when the user takes the next action and selects the physician that fits the searched parameters (here, Dr. Muneer M. Abidi who specializes in "oncology").

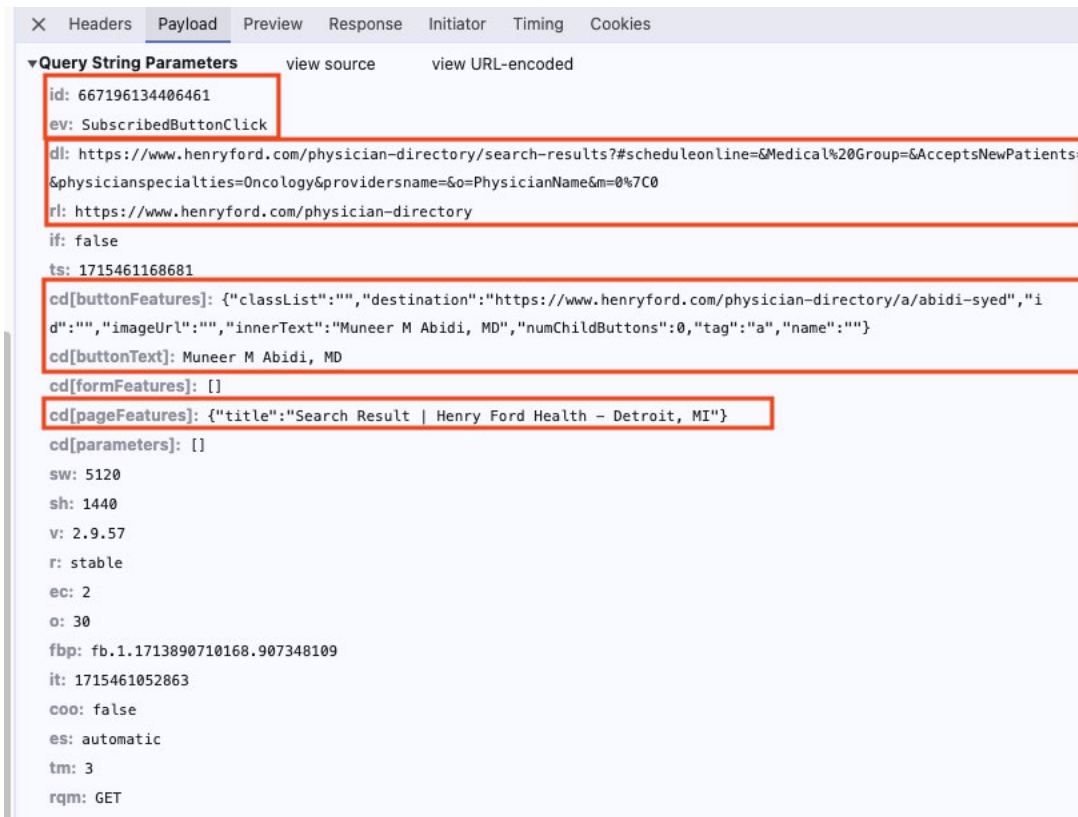


Figure 4. Screenshot taken from user's network traffic report during their physician search.

92. The first line of highlighted text, "id:367464206935045" refers to Defendant's Pixel ID and confirms that Defendant has downloaded the Facebook Pixel into its Source Code for this webpage.

93. On the same line of text, "ev= PageView," identifies and categorizes which actions the user took on the webpage ("ev=" is an abbreviation for event, and "PageView" is the type of event). Thus, this identifies the user as viewing the physician's page.

94. The additional lines of highlighted text show Defendant has disclosed to Facebook that the user: (1) is a patient seeking medical care from Defendant via <https://www.henryford.com/physician-directory/>; (2) is seeking treatment for cancer; and (3) is seeking treatment from this particular physician.

95. Finally, the highlighted text ("GET") demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's Facebook ID (c_user ID), thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.

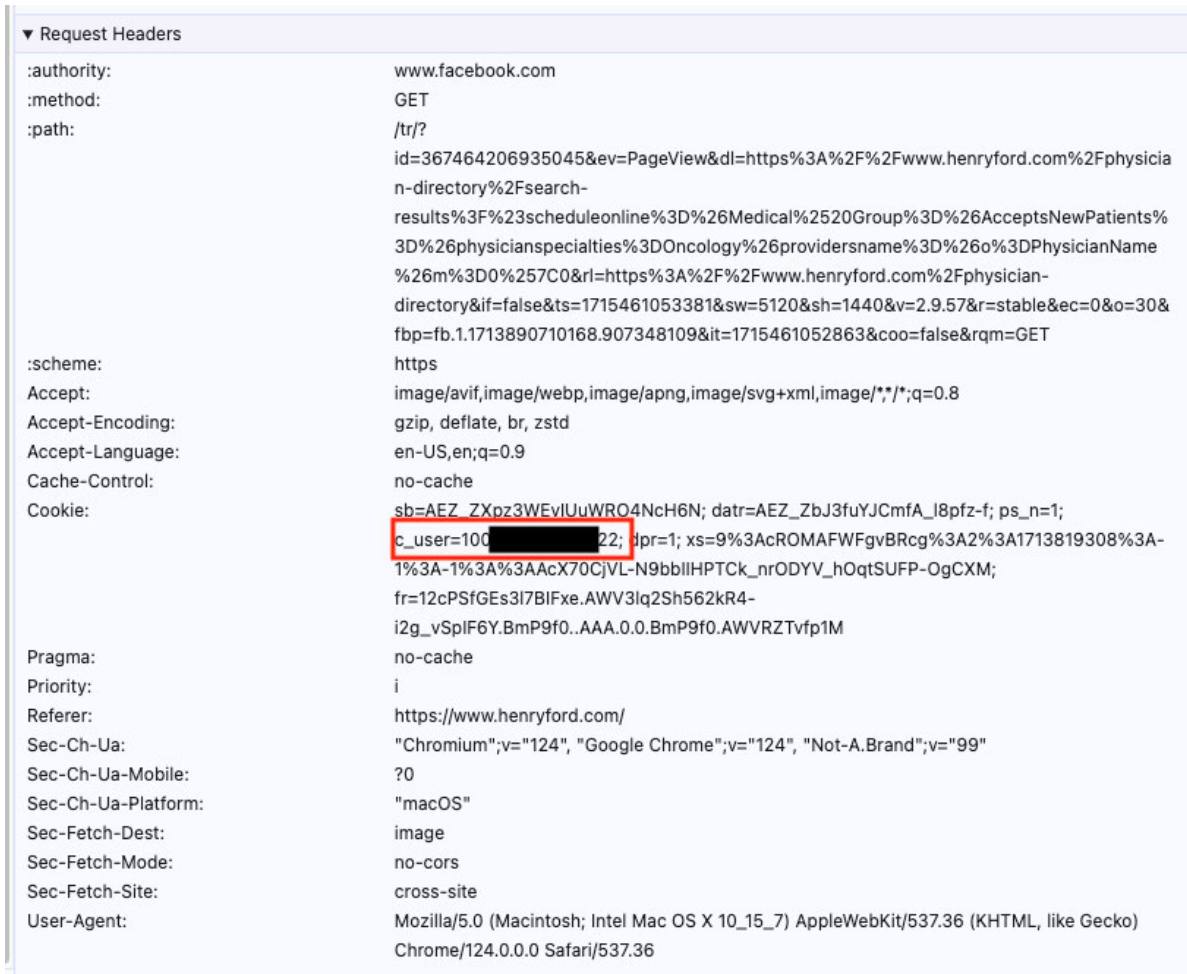


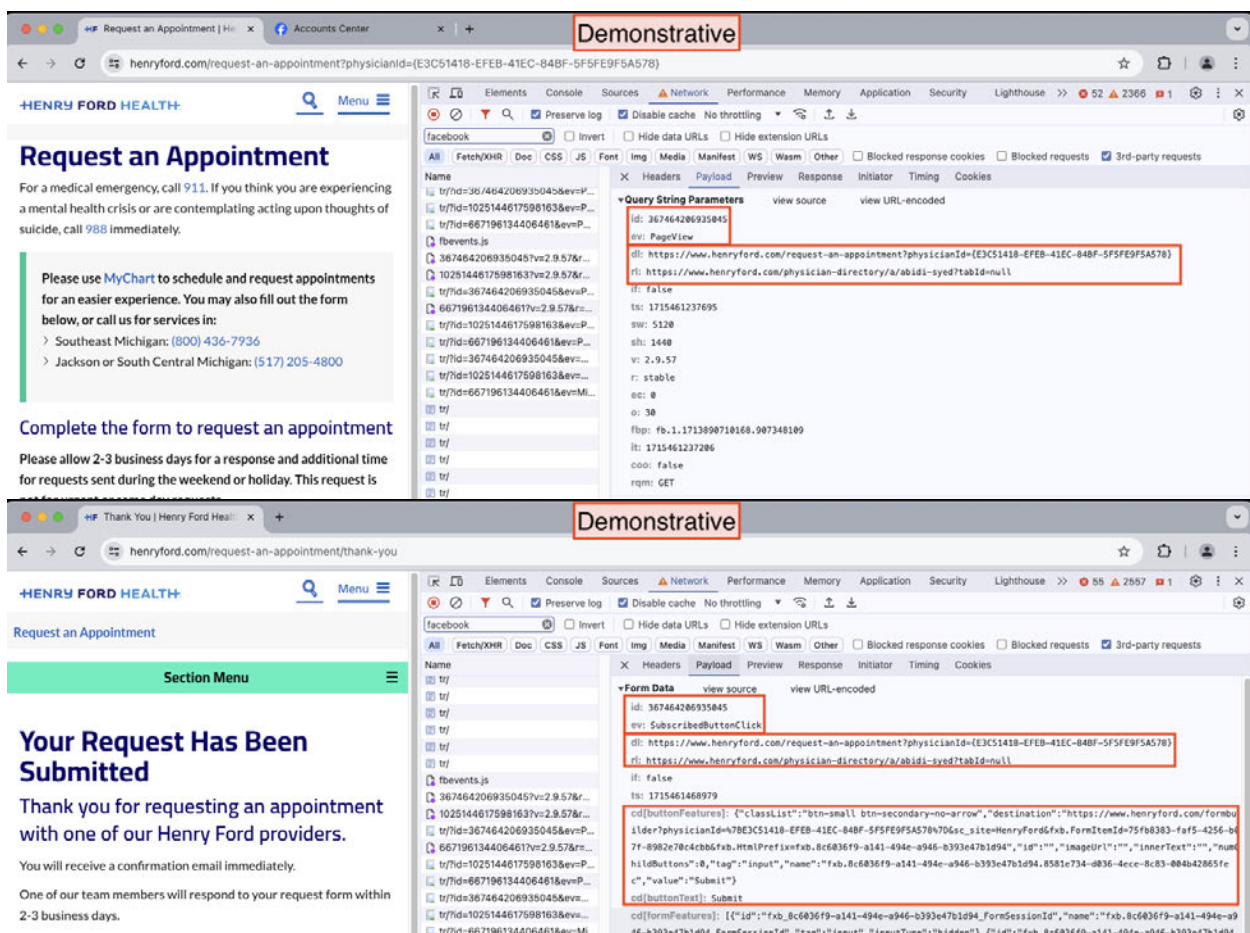
Figure 5. Screenshot of the details of the user's network traffic depicting the user's search results for a physician who specializes in oncology, along with the user's unique Facebook id.

96. The image demonstrates that the user's Facebook ID (highlighted as "c_user=" in the image above) was sent alongside the other data.³⁰

97. To make matters worse, Defendant's Facebook Pixel also shared with Facebook patients' appointment scheduling activities.

³⁰ The user's Facebook ID is represented as the c_user ID highlight in the image below, and Plaintiff has redacted the corresponding string of numbers to preserve the user's anonymity.

98. If, following the examples above, the user clicked a button on Defendant's webpage for Dr. Abidi to request an appointment, in addition to "PageView" and "Microdata" events sharing the user's activity on the webpage, Henry Ford transmitted a "SubscribedButtonClick" event informing Facebook that the patient clicked to "Submit" a form found on the "Request an Appointment" page.



Figures 6-7. Screenshots depicting disclosure of the fact that the user made an appointment with Dr. Abidi.

99. All of that information was sent to Facebook along with the user's personal identifiers, including their unique Facebook id:



Figure 8. Screenshot demonstrating disclosure of the user's appointment activity along with their *c_user* id cookie value.

100. The events in the images above contain the same physician ID, “E3C51418-EFEB-41EC-84BF-5F5FE9F5A578.” Plaintiff’s counsel’s research indicates that this physician ID is associated with Dr. Abidi. Therefore, Facebook had the information necessary to deduce that the user’s appointment request confirmation page was for Dr. Abidi.

101. Furthermore, in addition to appointments with specific physicians, Henry Ford also disclosed when users accessed their same-day care appointment tool.

102. Upon a user's click to access the Same-Day Care page, Henry Ford sent a "SubscribedButtonClick" event informing Facebook the user clicked "Same-day Care." Henry Ford confirmed the user loaded the next page through "PageView" and "Microdata" events which reveal that the user was learning about Henry Ford's "Same-Day Services | Primary Care."

103. As the user proceeded to select the type of same day care service they would like, Henry Ford would continue to inform Facebook about the user's activities. For example, when the user clicked to access a video visit, Henry Ford would send a SubscribedButtonClick event informing Facebook that the user clicked a button labeled "On-demand Video Visits." Henry Ford would subsequently send PageView and Microdata events as the next page loaded, informing Facebook that the user was learning about "Video Visits On Demand," which allowed them to "talk with a Henry Ford doctor on your phone, tablet or laptop."

104. To proceed to the on-demand video visit, the user would need to take the video visit via MyChart. If the user clicked to either access their appointment via MyChart, obtain instructions for the video visit, or create a MyChart account, Henry Ford would send a SubscribedButtonClick event informing Facebook that the user clicked to perform one of these tasks while they were on a page for "Video Visits on Demand."

105. Similarly, Henry Ford would inform Facebook when patients browsed Defendant's classes and events.

106. Upon a user's click to view Henry Ford's calendar page for its classes and events, Defendant would send a `SubscribedButtonClick` event. Once the calendar page for the classes and events loaded, Henry Ford would send a pair of `PageView` and `Microdata` events informing Facebook that the patients was on the page for "Classes and Events | Henry Ford Health | Henry Ford Health – Detroit, MI."

107. From the Classes and Events page, patients could conduct searches for relevant calendar events based on type and location. Henry Ford would report such patients' search parameters to Facebook.

108. For example, if a patient searched for childbirth and parenting events near the zip code 48202, Henry Ford would send `SubscribedButtonClick`, `PageView`, and `Microdata` events informing Facebook about the activity. The `PageView` and `Microdata` events reveal the patients' interest in "eventtype=childbirth and Parenting" near the location "zip=48202."

109. After patients searched for events, they have the option of browsing their results and booking attendance for certain events. As patients clicked to view their results and progressed through signing up for events, Henry Ford would report those activities to Facebook.

110. Continuing the example above in which the patients searched for childbirth and parenting related events, when the patients clicked to learn about a prenatal event from their search results, Henry Ford would send a SubscribedButtonClick event. The event informs Facebook that the patients clicked a button labeled “Great Expectations Prenatal Inperson,” from a page for “Upcoming Classes and Events | Henry Ford Health – Detroit, MI”:

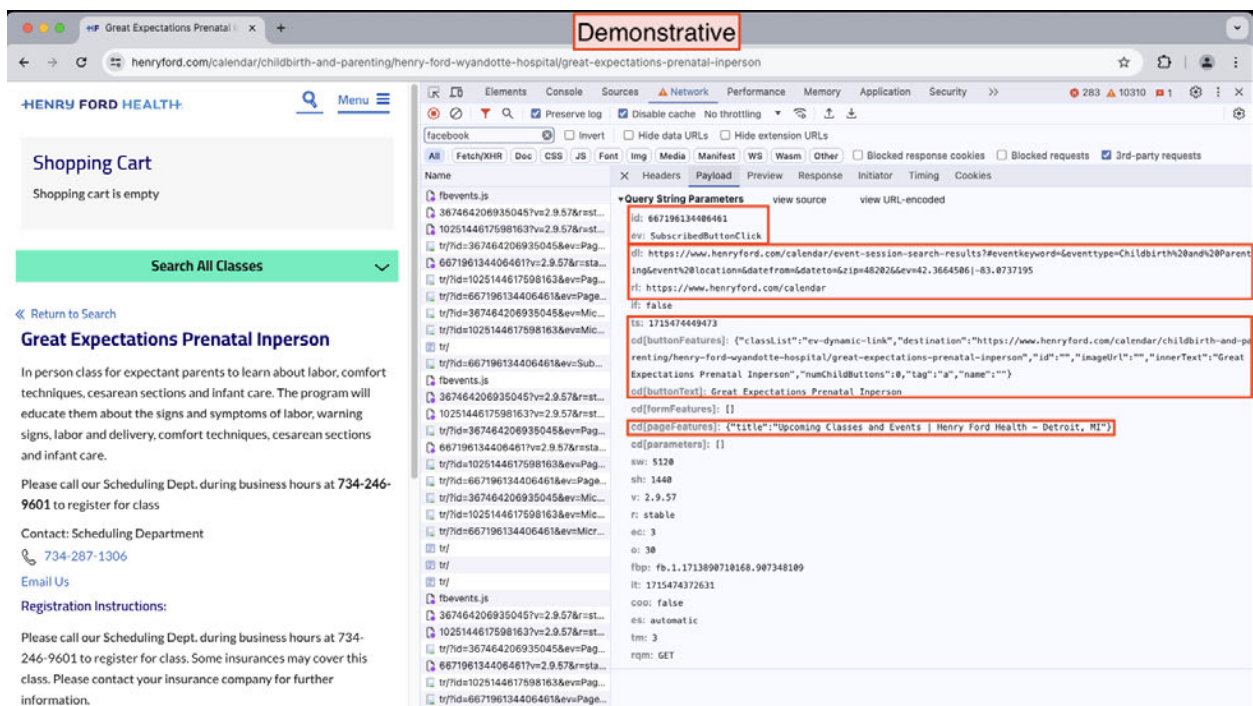


Figure 9. Defendant’s disclosure of the category of prenatal classes sought out by the patient.

111. Then, when the patients clicked to view a particular class on that page and added the event to their calendar, each such action would trigger Henry Ford to transmit a SubscribedButtonClick event. The events reveal that the patients clicked



43

attendance by filling out and submitting an event registration form, Henry Ford would send a series of `SubscribedButtonClick`, `PageView`, and `Microdata` events apprising Facebook of the user's progress.

113. As the page for the “Live Breastfeeding Class Online” West Bloomfield class loaded, Henry Ford would send `PageView` and `Microdata` events data to Facebook. When the patient clicked “I Want to Attend” the live breastfeeding class, Henry Ford transmitted a `SubscribedButtonClick` event informing Facebook about that activity. Next, when the patient clicked to submit their event registration form, Henry Ford sent another `SubscribedButtonClick` event, disclosing that the user clicked to “Checkout” after viewing a page with a calendar event for “live-breastfeeding-class,” *Figure 12*:

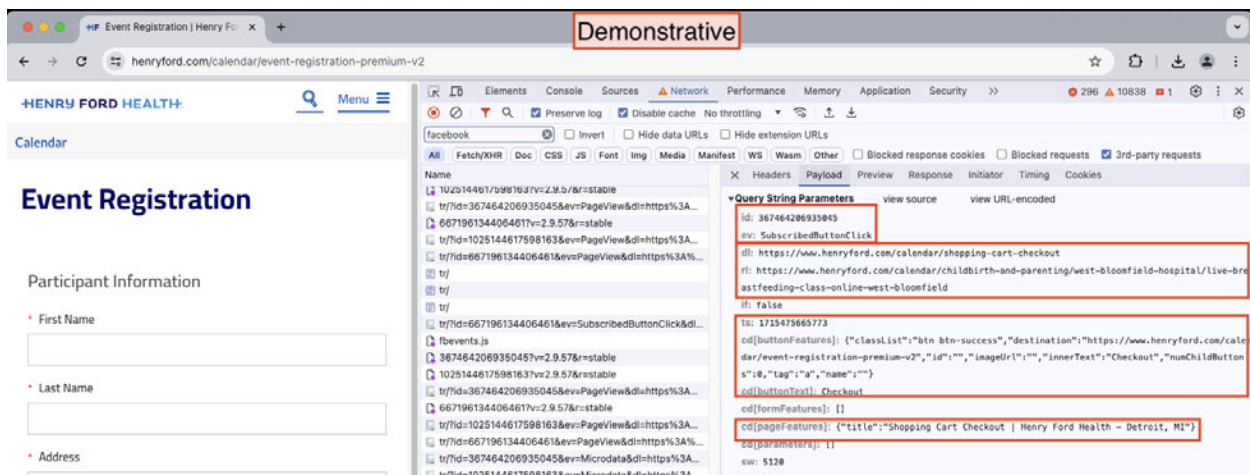


Figure 12: Screenshot of the Event Registration page for Live-Breastfeeding Class from Defendant's website.

114. From the next page, the patient must submit their billing information to reserve their spot in the class. After the patient added their payment information and

then clicked to pay, Henry Ford would send another `SubscribedButtonClick` event to Facebook, reporting that the patient clicked a button labeled “Enter payment Information.”

115. Henry Ford also shared with Facebook users’ activities that could reveal their status as patients. These types of activities include their pharmacy, bill pay, medical record requests, and MyChart activities.

116. For example, Defendant offers pharmacy services to its patients. As soon as a patient accessed Henry Ford’s pharmacy services page, Defendant would inform Facebook about this through `SubscribedButtonClick`, `PageView`, and `Microdata` events.

117. The `SubscribedButtonClick` event revealed that the patient clicked to access “Pharmacy,” and the `PageView` and `Microdata` events confirmed that the user loaded the page on <https://www.henryford.com/services/pharmacy>.

118. From the Pharmacy page, patients can click to (i) access retail prescriptions, (ii) access specialty medications and delivery services, or (iii) HFH’s pharmacy locations. When a patient clicked to view any of these options, Henry Ford would send a `SubscribedButtonClick` event revealing that the user clicked for “Retail Prescriptions[,] Specialty Medications and Free Delivery[, or] Pharmacy Locations.”

119. Additionally, Henry Ford disclosed patients’ bill pay related activities. Upon a user’s click to navigate to the Billing page, Henry Ford would transmit a

SubscribedButtonClick event informing Facebook that the patient clicked to “Pay Your Bill.” Next, as the Billing page loaded, Henry Ford would transmit PageView and Microdata events confirming that the user was on a page for “Billing” and that “Henry Ford provides many online resources for billing questions and is available to help over the phone and by mail.”

120. From the Billing page, the patient could pay via various methods. Henry Ford would transmit SubscribedButtonClick events informing Facebook when the patient selected to pay via the options presented. If the patient did not have a MyChart account and chose to pay as a guest, for example, Henry Ford would send a SubscribedButtonClick event revealing that the patient clicked to navigate to “Mychart/billing/guestpay.” If the user instead chose to pay via phone, Henry Ford would send a SubscribedButtonClick event informing Facebook that the user clicked to call “tel:1-800-999-5829,” on the Billing page.

121. Further, Henry Ford disclosed patients’ medical records related activities.

122. As soon as a patient clicked to navigate to the Medical Records page, Henry Ford would send a SubscribedButtonClick event, which informs Facebook that the user clicked a button labeled “Medical Records.” Then, Henry Ford would send a pair of PageView and Microdata events when the Medical Records page loaded. Both events confirm that the user was on the page

“https://www.henryfrod.com/visitors/records,” and the Microdata event further reveals that the user could learn “How to access your Henry ford Medical record,” on the page.

123. Once the patient was on the Medical Records page, Henry Ford would continue to disclose the user’s activities on the page. For example, the user could request medical records online or request a release form for a deceased patient’s records on the page. Each of these activities would trigger Henry Ford to send a SubscribedButtonClick event, which informed Facebook that the user clicked to “Request Medical Records,” or to download a “request-for-deceased-patient-records.pdf,” respectively.

124. Additionally, Henry Ford shared patients’ activities on its MyChart landing page, where users could click to log in, request assistance with logging in, or sign up and activate their MyChart accounts.

125. As a patient clicked to navigate to and loaded the MyChart landing page, Henry Ford would transmit PageView, and Microdata events. The events would reveal that the user is viewing the “MyChart | Henry Ford Health” page.

126. Henry Ford would continue to send events disclosing patients’ activities once they were on the MyChart landing page. For instance, when a user clicked to log in to MyChart, Henry Ford would send a SubscribedButtonClick event informing Facebook that the user clicked to “Log in to MyChart.”

127. If the patient, instead, needed assistance with a forgotten username or navigated to create a username or to activate their account, Henry Ford would similarly send a `SubscribedButtonClick` event for each activity, revealing that the patient clicked “Forgot your MyChart Username;” to “Sign up for MyChart;” or to “Activate your account,” respectively.

128. Finally, Defendant’s Tracking Tools even track and record the exact text and phrases that a user types into the general search bar located on Defendant’s homepage. In the example below, the user typed “cancer” into the search bar.

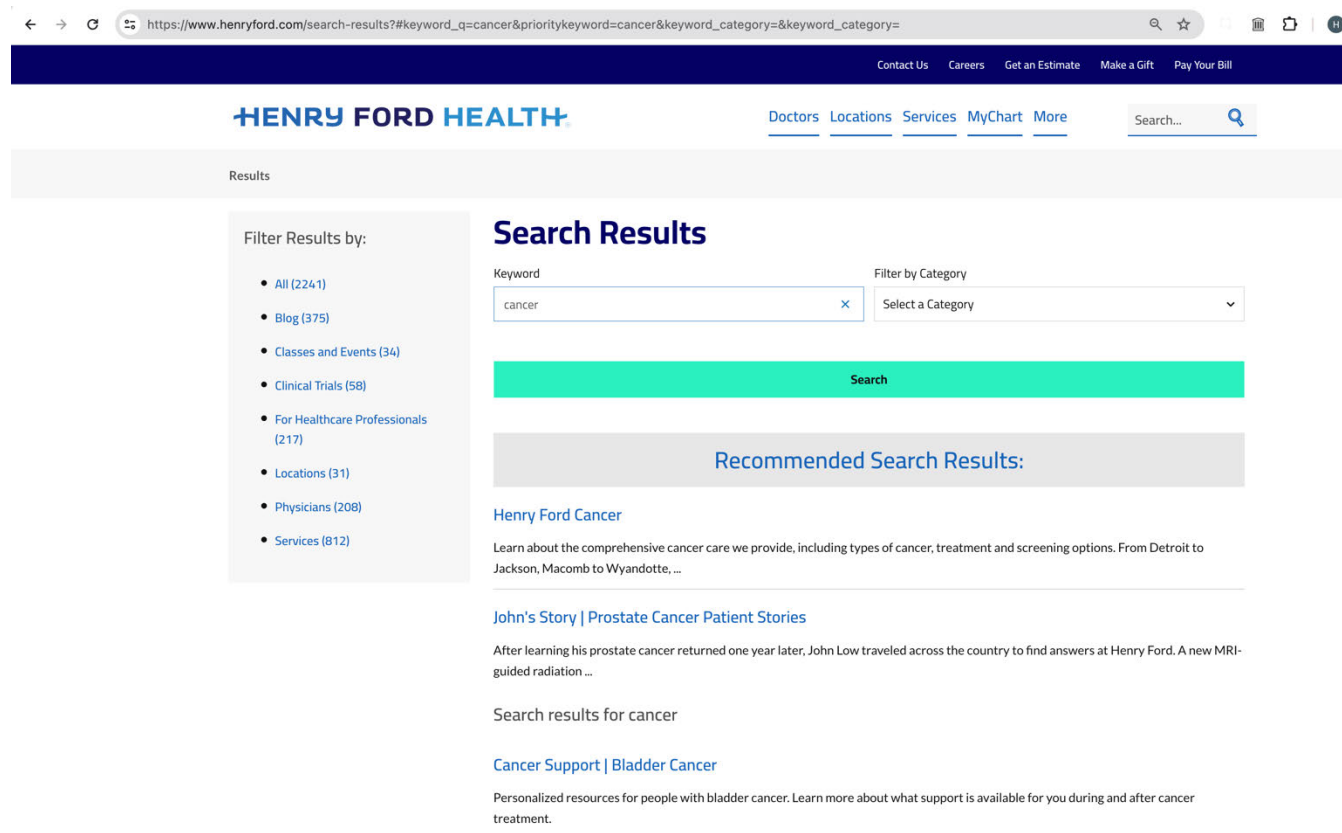


Figure 13. Defendant’s disclosure of the exact search terms typed by the user (“cancer”) into the Website’s search bar.

129. Resultantly, the exact search term is sent to Facebook, thereby allowing the patient's medical condition to be linked to their individual Facebook account for future retargeting and exploitation. This is simply unacceptable, and there is no legitimate reason for sending this information to Facebook.

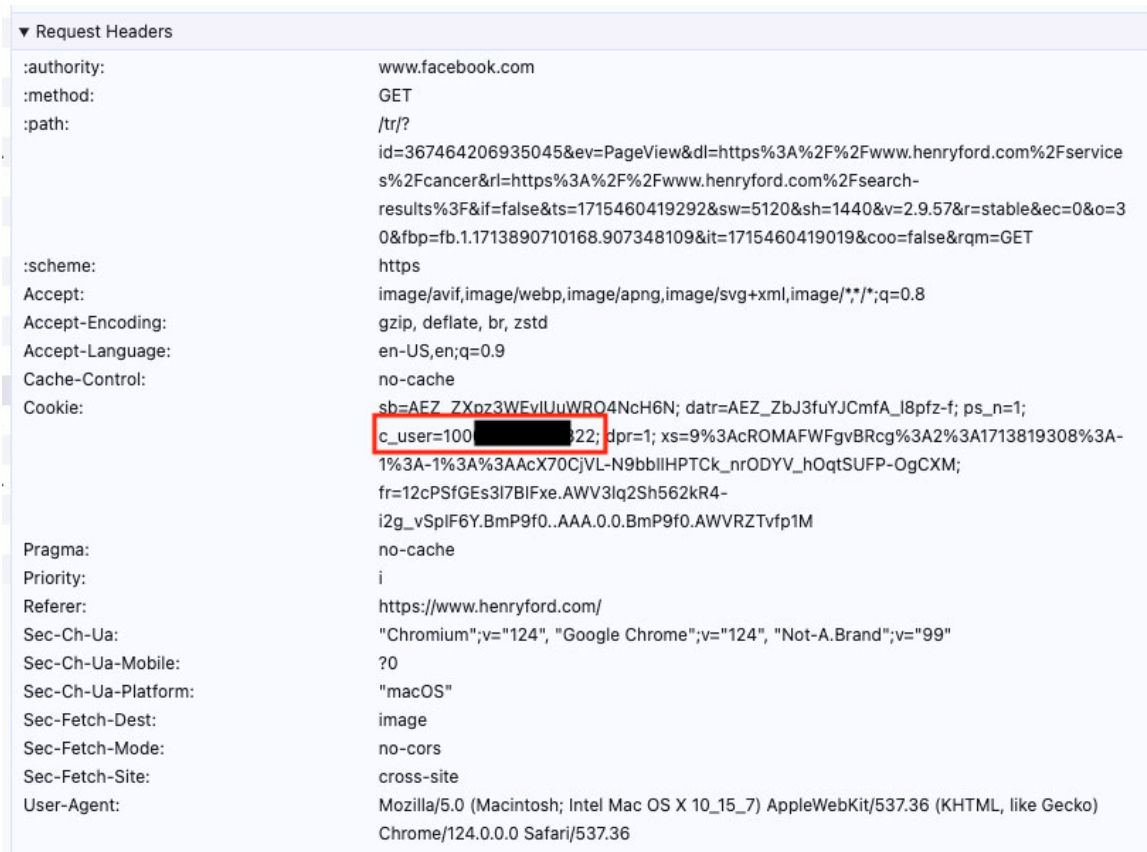
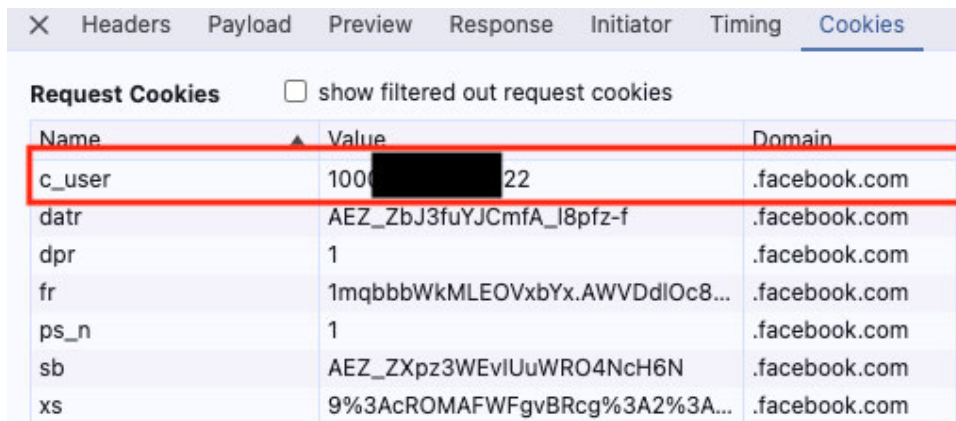


Figure 14. Screenshot taken from the user's traffic report depicting the details of the user's search along with their Facebook ID.

130. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook alongside their personally identifiable information. Several different methods allow marketers and third-parties to identify individual website users, but the examples above

demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

131. Facebook receives at least six cookies when Defendant's Website transmits information via the Pixel, *Figure 15*:



Name	Value	Domain
c_user	100[REDACTED]22	.facebook.com
datr	AEZ_ZbJ3fuYJCmfA_l8pfz-f	.facebook.com
dpr	1	.facebook.com
fr	1mqbbbWkMLEOVxbYx.AWVDdlOc8...	.facebook.com
ps_n	1	.facebook.com
sb	AEZ_ZXpz3WEvIUuWRO4NcH6N	.facebook.com
xs	9%3AcROMAFWFgVBRcg%3A2%3A...	.facebook.com

Figure 15: Screenshot of the cookies tab reflecting what cookies are sent via the Meta Pixel.

132. The fr cookie contains an encrypted Facebook ID and browser identifier.³¹ Facebook, at a minimum, uses the fr cookie to identify users, and this

³¹ Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit*, p. 33 (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited June 20, 2024).

particular cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.³²

133. The cookies listed in the two images above are commonly referred to as third-party cookies because they were “created by a website with a domain name other than the one the user is currently visiting”—i.e., Facebook. Although Facebook created these cookies, Defendant is ultimately responsible for the manner in which individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout its website.

134. Defendant also revealed its Website visitors' identities via first-party cookies such as the `_fbp` cookie that Facebook uses to identify a particular browser and a user, *Figure 16*:³³

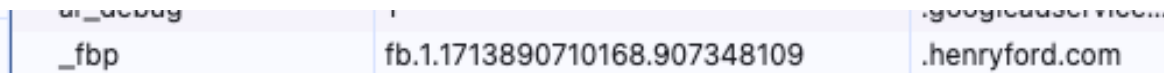


Figure 16: screenshot of the `_fbp` cookie directly associated with Defendant.

135. Importantly, the `_fbp` cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike

³² *Cookies & other storage technologies*, <https://www.facebook.com/policy/cookies/> (last visited June 20, 2024).

³³ *Id.*

the fr cookies and c_user cookie, the _fbp cookie functions as a first-party cookie— i.e. a cookie that was created and placed on the website by Defendant.³⁴

136. The Facebook Pixel uses both first- and third-party cookies.

137. Moreover, as seen in the image below, when patients visit <https://mychart.hfhs.org/MyChart/Authentication/Login> to login into their MyChart account on Defendant's Website, the Pixel is running on the login page and transmitting that the patient is logging into MyChart, *Figure 17*:

³⁴ The _fbp cookie is always transmitted as a first-party cookie.

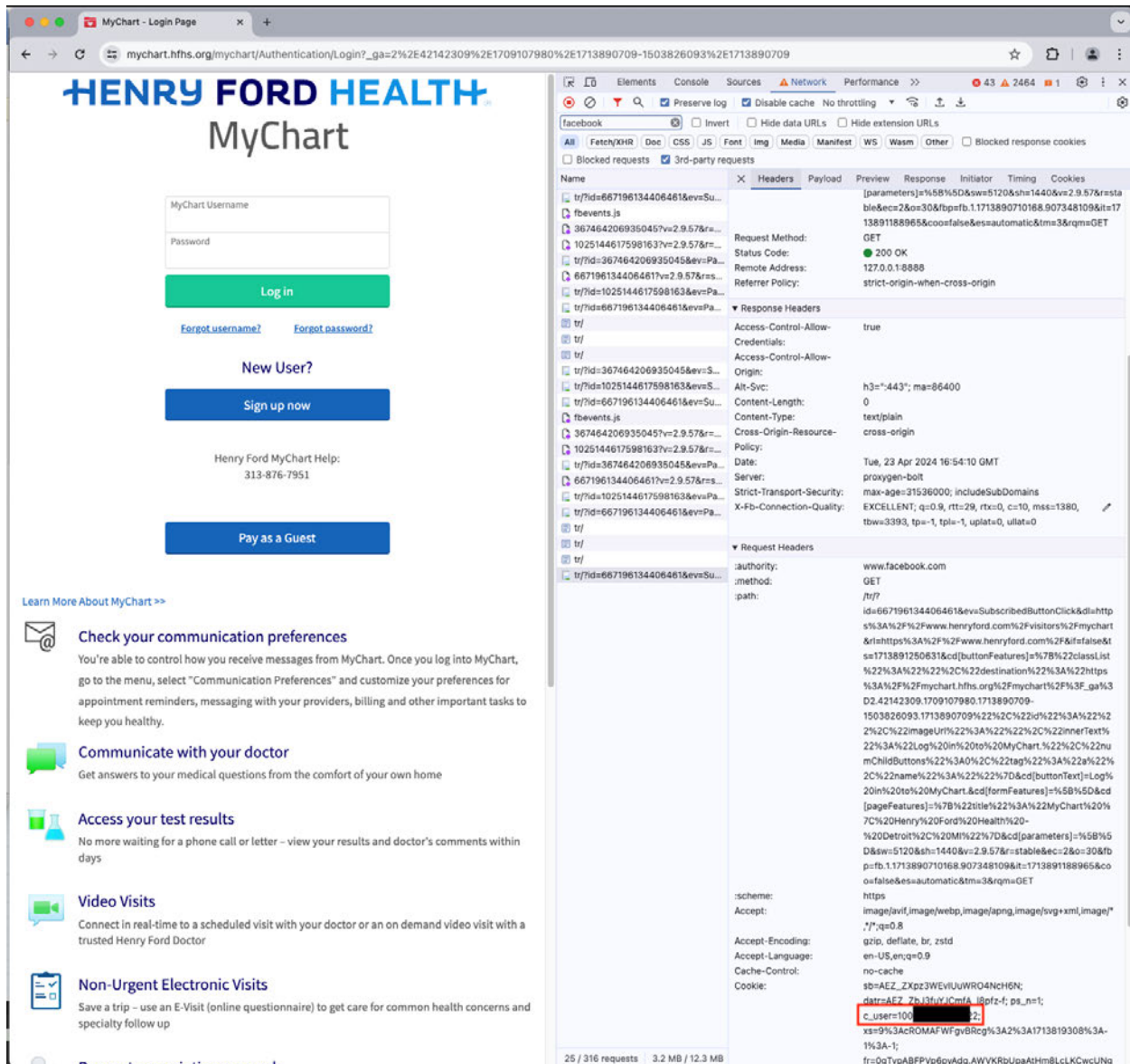


Figure 17: Screenshot of the Henry Ford Health MyChart login page depicting the Meta Pixel being present upon login.

138. In summation, Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, patients'

information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

139. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant has been using additional Tracking Tools to transmit its patients' Private Information to additional third parties. For example, Plaintiff's counsels' investigation revealed that Defendant was also sending its patients' protected health information to Google via Google tracking tools including Google Analytics, DoubleClickAds, and Google Tag Manager.

140. Defendant does not disclose that the Pixel, Google trackers, first-party cookies from third parties like Facebook and/or Google, or any other Tracking Tools embedded in the Website's source code track, record, and transmit Plaintiff's and Class Members' Private Information to Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose Plaintiff's and Class Members' private communications to Facebook or Google.

F. Plaintiff Nina McClain's Experience

141. Plaintiff has been a patient of Defendant for more than ten years and has utilized Defendant's Website since at least 2011.

142. As detailed herein, Plaintiff accessed Defendant's Website on her computer and mobile device and used the Website to look for providers, review conditions and treatments, make appointments and communicate with her providers.

143. As a condition of receiving Defendant's services, Plaintiff disclosed her Private Information to Defendant on numerous occasions, and most recently in February of 2024.

144. Plaintiff accessed Defendant's Website and Patient Portal on her phone and laptop to receive healthcare services from Defendant and at Defendant's direction.

145. Plaintiff has maintained an active Facebook account throughout the relevant period in this case, which she is perpetually logged into and which is registered under her legal name.

146. During the relevant time period, when the Defendant's Pixels were present, and specifically in May 2017 through June 2017, and May 2020 through November 2020, when Plaintiff [REDACTED] she used Defendant's Website, <https://www.henryford.com/>, to research [REDACTED], including [REDACTED] [REDACTED], what it means to [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]), and look for Defendant's locations close to her address.

147. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications

about Plaintiff's prospective healthcare providers. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

<https://www.henryford.com/locations/woodhaven>

<https://www.henryford.com/physician-directory/search-results?|#q=&physicianspecialties=&providersname=&scheduleonline=&medical%20group=&acceptsnewpatients=&physicianlocations=Henry%20Ford%20Medical%20Center%20-%20Woodhaven&gender=&zip=&languages%20spoken=&hospital%20affiliations=&o=PhysicianName&m=0|0&e=0>

[https://www.henryford.com/search-](https://www.henryford.com/search-results?#keyword_q=[REDACTED])

[results?#keyword_q=\[REDACTED\]](https://www.henryford.com/search-results?#keyword_q=[REDACTED])

[https://www.henryford.com/physician-directory/search-results?#q=&physicianspecialties=\[REDACTED\]&providersname=&scheduleonline=&medical%20group=&acceptsnewpatients=&physicianlocations=Henry%20Ford%20Medical%20Center%20-%20Woodhaven&gender=Female&zip=&languages%20spoken={42DF66A5-A640-4FED-A82F-05CD431E3B38}&hospital%20affiliations=&o=PhysicianName&m=0|0&e=0](https://www.henryford.com/physician-directory/search-results?#q=&physicianspecialties=[REDACTED]&providersname=&scheduleonline=&medical%20group=&acceptsnewpatients=&physicianlocations=Henry%20Ford%20Medical%20Center%20-%20Woodhaven&gender=Female&zip=&languages%20spoken={42DF66A5-A640-4FED-A82F-05CD431E3B38}&hospital%20affiliations=&o=PhysicianName&m=0|0&e=0)

[https://www.henryford.com/physician-directory/search-results?#scheduleonline=&medical%20group=&acceptsnewpatients=&physicianspecialties=\[REDACTED\]&providersname=&o=PhysicianName&m=0|0&e=0](https://www.henryford.com/physician-directory/search-results?#scheduleonline=&medical%20group=&acceptsnewpatients=&physicianspecialties=[REDACTED]&providersname=&o=PhysicianName&m=0|0&e=0)

148. Contemporaneously with the interception and transmission of Plaintiff's communications on <https://www.henryford.com/>, Defendant also disclosed to Meta Plaintiff's personal identifiers, including but not limited to her IP address and Facebook ID.

149. Plaintiff reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

150. Plaintiff provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law

151. Further to the systematic process described herein, Defendant assisted Facebook with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information and related confidential information.

152. Defendant assisted these interceptions without Plaintiff's knowledge, consent or express written authorization.

153. Following her visits to Defendant's Website, Plaintiff observed advertisements on her Facebook account related to the treatments she sought and received through medical providers she viewed on Defendant's Website, specifically [REDACTED]

154. Plaintiff submitted medical information to Defendant via its Website. Because Defendant utilizes the Facebook Pixel, the Website's Source Code sends a secret set of instructions back to the individual's browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and both the webpage's and, upon information and belief, MyChart portal's URLs to Facebook.

155. Pursuant to the systematic process described in this Complaint, Plaintiff's Private Information was disclosed to Facebook, and this data included her PII, PHI, and related confidential information. Defendant intercepted and/or assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

156. As Defendant's patient, Plaintiff reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted to or disclosed to a third party. But

for her status as Defendant's patient, Plaintiff would not have disclosed her Private Information to Defendant.

157. During her time as a patient, Plaintiff never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

158. Notwithstanding, through the Pixel, other Tracking Tools and Conversions API, Defendant transmitted Plaintiff's Private Information to third parties, such as Facebook and Google.

159. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' FIDs, IP addresses, and/or device IDs or other information they input into Defendant's Website, like their home address, zip code, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients. Plaintiff's and Class Members identities could be easily determined based on the FID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

160. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies

their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

161. Based on the presence of the Pixel and Conversions API, Defendant unlawfully disclosed Plaintiff's Private Information to Facebook. The presence of Facebook advertisements confirms Defendant's unlawful transmission of Plaintiff's Private Information to Facebook. Said differently, Plaintiff did not disclose this Private Information to any other source—only Defendant's Website.

162. In sum, Defendant's Pixel transmitted Plaintiff's highly sensitive communications and Private Information to Facebook, including communications that contained private and confidential information, without Plaintiff's knowledge, consent, or express written authorization

163. Defendant breached Plaintiff's right to privacy and unlawfully disclosed her Private Information to Facebook. Specifically, Plaintiff had a reasonable expectation of privacy, based on her status as Defendant's patient, that Defendant would not disclose her Private Information to third parties.

164. Defendant did not inform Plaintiff that it shared her Private Information with Facebook.

165. By doing so without Plaintiff's consent, Defendant breached Plaintiff's and Class Members' right to privacy and unlawfully disclosed Plaintiff's Private Information.

166. Upon information and belief, as a "redundant" measure to ensure Plaintiff's Class Members' Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's and Class Members' Private Information from electronic storage on Defendant's server directly to Facebook.

167. Plaintiff suffered injuries in the form of (i) invasion of privacy; (ii) diminution of value of the Private Information; (iii) statutory damages; (iv) the continued and ongoing risk to her Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff's medical conditions and other confidential information she communicated to Defendant via the Website.

168. Plaintiff has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

G. Defendant's Conduct Is Unlawful and Violated Industry Norms

i. Defendant Violated HIPAA Standards

169. Under federal law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients’ express written authorization.³⁵

170. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, “establishes national standards to protect individuals’ medical records and other individually identifiable health information (collectively defined as ‘protected health information’) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.”³⁶

171. The Privacy Rule broadly defines “protected health information” (“PHI”) as individually identifiable health information (“IIHI”) that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

172. IIHI is defined as “a subset of health information, including demographic information collected from an individual” that is: (1) “created or

³⁵ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

³⁶ HIPAA For Professionals (last visited June 18, 2024), <https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html>.

received by a health care provider, health plan, employer, or health care clearinghouse”; (2) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual”; and (3) either (a) “identifies the individual” or (b) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

173. Under the HIPAA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination”; or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

a. Names;

H. Medical record numbers;

J. Account numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; ... and

R. Any other unique identifying number, characteristic, or code...;and”

The covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”

45 C.F.R. § 160.514.

174. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

175. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

176. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

177. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

178. In Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS instructs:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.³⁷

³⁷https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredenities/De-identification/hhs_deid_guidance.pdf (last visited June 18, 2024).

179. In its guidance for Marketing, the HHS further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual’s written authorization before a use or disclosure of his or his protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.* (Emphasis added).³⁸

180. As alleged above, there is an HHS Bulletin that highlights the obligations of “regulated entities,” which are HIPAA-covered entities and business associates, when using tracking technologies.³⁹

181. The Bulletin expressly provides that “[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.”

182. Defendant’s actions violated HIPAA Rules.

³⁸<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredenities/marketing.pdf> (last visited June 18, 2024).

³⁹ See <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

ii. Defendant Violated Michigan Law

183. Michigan law has established policies and procedures for the maintenance, preservation, and storage of patient medical records.

184. Michigan law provides that all patients are entitled to privacy and confidentiality with respect to their treatment and medical records: “a health care corporation shall not disclose records containing personal data that may be associated with an identifiable member, or personal information concerning a member, to a person other than the member, without the prior and specific informed consent of the member to whom the data or information pertains. The member's consent shall be in writing.” MCL 550.1406(1).

185. Michigan law also provides that medical professionals are not allowed to disclose information obtained from a patient: “a health care corporation shall make a disclosure for which prior and specific informed consent is not required upon the condition that the person to whom the disclosure is made protect and use the disclosed data or information only in the manner authorized by the corporation..... If a member has authorized the release of personal data to a specific person, a health care corporation shall make a disclosure to that person upon the condition that the person shall not release the data to a third person unless the member executes in writing another prior and specific informed consent authorizing the additional release.” MCL 550.1406(1).

186. Defendant's actions described herein violated Michigan law.

iii. Defendant Violated Industry Standards

187. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

188. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

189. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)

190. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

191. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically...must...(c) release patient information only in keeping ethics guidelines for confidentiality.

H. Plaintiff's and Class Members' Expectation of Privacy

192. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

193. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

194. Plaintiff and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

I. Unique Personal Identifiers Are PII

195. While not all health data is covered under HIPAA, the law specifically applies to healthcare providers, health insurance providers and healthcare data clearinghouses.⁴⁰

196. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered personally identifiable information (“PII”). This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

197. These HIPAA Identifiers, as relevant here, include names, dates related to an individual, email addresses, device identifiers, web URLs and IP addresses.⁴¹

⁴⁰ See Alfred Ng & Simon Fondrie-Teitler, *This Children’s Hospital Network Was Giving Kids’ Information to Facebook*, The Markup (June 21, 2022), <https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook> (stating that “[w]hen you are going to a covered entity’s website, and you’re entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there’s a strong possibility that HIPAA is going to apply in those situations”).

⁴¹ *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited June 14, 2024).

198. Unique personal identifiers become PHI when they can be associated with personal health information.⁴²

199. Henry Ford improperly disclosed Plaintiff's and Class Members' HIPAA identifiers, including their names, emails, dates they sought treatments, computer IP addresses, device identifiers and web URLs visited to Facebook and Google through their use of the Pixels in addition to services selected, patient statuses, medical conditions, treatments, provider information and appointment information.

200. An IP address is a number that identifies the address of a device connected to the Internet. IP addresses are used to identify and route communications on the Internet. IP addresses of individual Internet users are used by Internet service providers, websites and third-party tracking companies to facilitate and track Internet communications.

201. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

⁴² *See id.* (“[p]rotected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.”).

202. Facebook, Google and other third-party marketing companies track IP addresses to target individual homes and their occupants with advertising.

203. Under HIPAA, an IP address is considered personally identifiable information, which is defined as including “any unique identifying number, characteristic or code” and specifically listing IP addresses among examples. See 45 C.F.R. § 164.514 (2).

204. HIPAA further declares information as personally identifiable where the covered entity has “actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

205. Consequently, Henry Ford’s disclosure of Plaintiff’s and Class Members’ IP addresses violated HIPAA and industry-wide privacy standards because it was connected to their past, present, or future medical conditions and treatment.

J. Defendant Was Enriched and Benefitted from the Use of The Tracking Tools and Unauthorized Disclosures

206. The primary motivation and a determining factor in Defendant’s interception and disclosure of Plaintiff’s and Class Members’ Private Information was to commit criminal and tortious acts in violation of federal and state laws as

alleged herein, namely, the use of patient data for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

207. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

208. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence of express written consent.

209. By utilizing the Tracking Tools, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiff and Class Members and violating their rights under federal and Michigan law.

K. Plaintiff's and Class Members' Private Information Had Financial Value

210. Plaintiff's data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as

Lookalike Audiences and then sells that information to advertising clients. Google has recognized the value of user data and has even instituted a pilot program in which it pays users \$3 per week to track them online.

211. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the “new oil.” Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200 billion industry wide.

212. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled “How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.⁴³

213. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole

⁴³ See <https://time.com/4588104/medical-data-industry/> (last visited June 18, 2024).

market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”⁴⁴

TOLLING

214. Any applicable statute of limitations has been tolled by the “fraudulent concealment” rule. Plaintiff did not know (and had no way of knowing) that her PII and PHI was intercepted and unlawfully disclosed to Facebook because Defendant affirmatively prevented its patients from learning these facts.

CLASS ACTION ALLEGATIONS

215. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated (“the Class”) pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

216. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, used Defendant’s Website and had their Private Information disclosed to a third party without authorization.

217. Plaintiff also seeks to represent a Michigan Subclass defined as:

All individuals residing in Michigan who are, or were, patients of Defendant or any of its affiliates, used Defendant’s Website, and had their Private Information disclosed to a third party without

⁴⁴ See <https://www.cnn.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited June 18, 2024).

authorization or consent.

The Nationwide Class and the Michigan Subclass are collectively referred to as the “Class.”

218. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

219. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

220. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant’s records.

221. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

- b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;
- d. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- g. Whether Defendant's conduct violated the MCPA, MCL 445.903;
- h. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages because of Defendant's wrongful conduct; and
- i. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of Defendant's disclosure of their Private Information.

222. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information

compromised because of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

223. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

224. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could

afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

225. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2).

This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

226. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each

Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

227. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

228. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

229. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

230. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief regarding the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

231. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, issues are appropriate for certification because such claims present only particular, common

issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to, the following:

- a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;
- f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief because of Defendant's wrongful conduct.

COUNT I

BREACH OF FIDUCIARY DUTY/CONFIDENTIALITY (On Behalf of Plaintiff and the Class)

232. Plaintiff incorporates all prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

233. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

234. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

235. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members: (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) to maintain complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

236. Contrary to its duties as a medical provider and its express and implied promises of confidentiality, Defendant installed its Tracking Tools to disclose and

transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

237. These disclosures were made for commercial purposes without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

238. The unauthorized disclosures of Plaintiff's and Class Members' Private Information were intentionally caused by Defendant's employees acting within the scope of their employment. Alternatively, the disclosures of Plaintiff's and Class Members' Private Information occurred because of Defendant's negligent hiring or supervision of its employees, its failure to establish adequate policies and procedures to safeguard the confidentiality of patient information, or its failure to train its employees to properly discharge their duties under those policies and procedures.

239. The third-party recipients included, but may not be limited to, Facebook and Google. Such information was received by these third parties in a manner that allowed them to identify the Plaintiff and the individual Class Members.

240. Defendant's breach of the common law implied covenant of trust and confidence is evidenced by its failure to comply with federal and state privacy regulations, including:

- a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

- b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- c. By failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);
- d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiff's and Class Members PHI;
- e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. By failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);
- g. By impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;
- h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);
- i. By failing to keep Private Information confidential as required by MCL 333.20201; and
- j. By otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

241. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

242. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and
- i. Defendant's actions violated the property rights Plaintiff and Class members have in their Private Information.

COUNT II
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
("ECPA")
18 U.S.C. § 2511(1) *et seq.*
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiff and the Class)

243. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

244. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

245. The ECPA protects both sent and received communications.

246. The ECPA, specifically 18 U.S.C. § 2520(a), provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed or intentionally used in violation of Chapter 119.

247. The transmissions of Plaintiff's and Class Members' Private Information to Henry Ford via Henry Ford's Website is a "communication" under the ECPA's definition under 18 U.S.C. § 2510(12).

248. The transmission of Private Information between Plaintiff and Class Members and Henry Ford via their Website is "transfer[s] of signs, signals, writing,

... data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

249. The ECPA defines “content” when used with respect to electronic communications to “include[] any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

250. The ECPA defines “interception” as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents ... include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

251. The ECPA defines “electronic, or other device” as “any device ... which can be used to intercept a[n] ... electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. The cookies Defendant, Meta and Google use to track Plaintiff’s and Class Members’ communications;
- b. Plaintiff’s and Class Members’ browsers;
- c. Plaintiff’s and Class Members’ computing devices;
- d. Henry Ford’s web-servers and

- e. The Pixels and other Tracking Tools deployed by Henry Ford to effectuate the sending and acquisition of users' and patients' sensitive communications.

252. Plaintiff and Class Members' interactions with Henry Ford's Website are electronic communications under the ECPA.

253. By utilizing and embedding the Pixels and Conversions API on their Website and/or servers, Henry Ford intentionally intercepted, endeavored to intercept and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

254. Specifically, Henry Ford intercepted Plaintiff's and Class Members' electronic communications via the Tracking Tools and Conversions API, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook and/or Google.

255. Furthermore, Defendant intercepted the "contents" of Plaintiff's communications in at least the following forms:

- a. The parties to the communications;
- b. PII such as patients' IP addresses, Facebook IDs, cid parameter cookie, browser fingerprints and other unique identifiers;
- c. The precise text of patient communications about specific medical conditions;
- d. The details of information generated when patients requested or made appointments,

- e. The details of information generated when patients signed up for classes;
- f. The details of patient communications about billing and payment;
- g. The precise dates and times when patients click to Log-In on Defendant's Website.

256. Henry Ford intercepted communications that included, but are not limited to, communications to/from Plaintiff and Class Members regarding Private Information, including their unique personal identifiers such as their Facebook ID, IP address, other unique personal identifiers and health information relevant to the appointments and classes in which Plaintiff and Class Members participated.

257. Defendant's acquisition of patient communications that were used and disclosed to Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and Michigan, including.

- a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
- b. Violation of MCL 333.20201(2)(c);
- c. Violation of MCL 550.1406;
- d. Violation of MCL 445.903 and
- e. Invasion of Privacy.

258. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Tools embedded and operating on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiff's and Class Members' electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

259. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Tools embedded and operating on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and Class Members' electronic communications, for purposes other than providing health care services to Plaintiff and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

260. Under Michigan's Public Health Code, MCL §333.20201(2)(d), "A patient or resident is entitled to privacy, to the extent feasible, in treatment and in caring for personal needs with consideration, respect, and full recognition of his or her dignity and individuality."

261. Defendant violated Michigan's Public Health Code by disclosing Plaintiff's and Class Members' Private Information to third parties without authorization or consent.

262. Under Michigan's Nonprofit Health Care Corporation Reform Act MCL §550.1406(1), "a health care corporation shall not disclose records containing personal data that may be associated with an identifiable member, or personal information concerning a member, to a person other than the member, without the prior and specific informed consent of the member to whom the data or information pertains. The member's consent shall be in writing."

263. Defendant violated Michigan's Nonprofit Health Care Corporation Reform Act MCL §550.1406(1) by disclosing Plaintiff's and Class Members' Private Information to third parties without authorization or consent

264. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Tools it embedded and operated on its Website, contemporaneously and intentionally redirected the contents of Plaintiff's and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

265. Henry Ford intentionally used wire or electronic communications to increase its profit margins. Henry Ford specifically used the Tracking Tools and

Conversions API to track and utilize Plaintiff's and Class Members' Private Information for its own financial benefit.

266. Henry Ford was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communications.

267. Plaintiff and Class Members did not authorize Henry Ford to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy via the Tracking Tools including the Pixels and Conversions API.

268. Any purported consent that Henry Ford received from Plaintiff and Class Members was not valid.

269. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State—namely, violations of HIPAA and invasion of privacy, among others.

270. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

271. Defendant is a “party to the communication” with respect to patient communications. However, Defendant's simultaneous, unknown duplication,

forwarding and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

272. In sending and acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Henry Ford's Website, looking up specific providers and/or treatments, scheduling appointments, and registering for healthcare classes, Henry Ford's purpose was tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, conversation or matter that would be highly offensive to a reasonable person.

273. Henry Ford's acquisition of patient communications that were used and disclosed to Facebook and other third parties was also done for purposes of committing criminal and tortious acts in violation of the laws of the United States and Michigan (as described *infra*) as well as various common law causes of action.

274. Additionally, through the above-described tracking technologies and intercepted communications, this information was, in turn, used by Facebook and Google to 1) place Plaintiff in specific health-related categories and 2) target Plaintiff with particular advertising associated with Plaintiff's specific health conditions.

275. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted,

shared, and used their individually-identifiable patient health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;

- b. Defendant received substantial financial benefits from its use of Plaintiff's and Class Members' individually-identifiable patient health information without providing any value or benefit to Plaintiff or the Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' individually-identifiable patient health information, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiff or the Class Members;
- d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and
- e. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and

confidential information, such as patient status, test results, and appointments that Plaintiff and Class Members intended to remain private no longer private.

276. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT III
INVASION OF PRIVACY
Violations of MCL 750.539j
(On Behalf of Plaintiff and the Class)

277. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

278. Plaintiff and Class Members have a statutory privacy interest in their names, portraits, pictures, and voices under Michigan Law .

279. Defendant knowingly used Plaintiff's and Class Members' names and other Private Information in the State of Michigan for advertising and trade purposes without first obtaining their written consent.

280. Specifically, Defendant transmitted Plaintiff's and Class Members' names and/or FID to third parties like Facebook for targeted advertising and other commercial purposes, as described herein.

281. Defendant's use of Plaintiff's and Class Members' names and Private Information did not serve any public interest.

282. The unlawful tracking of Plaintiff and Class Members' and disclosure of their names in connection with their Private Information has caused Plaintiff and Class Members to suffer damages. This includes damage to the value of their information, which Defendant appropriated for its own enrichment. Plaintiff and Class Members have also suffered nominal damages.

283. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it installed Tracking Tools onto its Website because the purpose of the Tracking Tools is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

284. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

285. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the

privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs. Alternatively, Plaintiff and Class Members are entitled to nominal damages.

286. Plaintiff and Class Members are entitled to exemplary and/or punitive damages because of Defendant's knowing violations of their statutory rights to privacy.

287. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and still in the possession of Facebook and other third parties and the wrongful disclosure of the information cannot be undone.

288. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

289. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into Plaintiff's and Class Members' statutory privacy interests.

COUNT IV
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff and the Class)

290. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

291. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and the Class Members provided their Private Information and compensation for their medical care.

292. When Plaintiff and Class Members provided their Private Information to Defendant, they entered an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

293. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

294. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

295. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties like Facebook or Google.

296. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

297. Plaintiff and Class Members are entitled to compensatory and consequential damages because of Defendant's breach of implied contract.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

298. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class and pleads this Count in the alternative.

299. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

300. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

301. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with

economic, intangible, and other benefits, including substantial monetary compensation.

302. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

303. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

304. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VI
NEGLIGENCE
(On behalf of Plaintiff and the Class)

305. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

306. Defendant owed Plaintiff and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

307. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

308. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

309. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

310. The third-party recipients included, but may not be limited to, Facebook and/or Google.

311. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;

- b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and
- i. Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

COUNT VII
VIOLATIONS OF THE MICHIGAN NONPROFIT HEALTH CARE
CORPORATION REFORM ACT
MCL 550.140 *et seq.*
(On behalf of Plaintiff and the Michigan Subclass)

312. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

313. This cause of action is brought pursuant to the Michigan Nonprofit Health Care Corporation Reform Act (the "Reform Act"), MCL § 550.140, which

requires in relevant part that a Michigan nonprofit healthcare corporation “use reasonable care to secure” members’ healthcare records “from unauthorized access” and thereby “ensure the confidentiality of records containing personal data that may be associated with identifiable members.” MCL 550.1406(1).

314. As a nonprofit healthcare corporation incorporated in the State of Michigan and providing healthcare and hospital services in the State, Henry Ford is and was at all relevant times a “healthcare corporation” as that term is defined in MCL §§ 550.1105(2) and 50.1406.

315. As a person entitled to receive healthcare under a nongroup insurance certificate while obtaining healthcare from Henry Ford, Plaintiff is and was at all relevant times a “member” as that term is defined in MCL §§ 550.1106(3) and 50.1406.

316. By the acts alleged above, Henry Ford violated the Reform Act by failing to adequately safeguard Plaintiff’s PII/PHI from unauthorized access by third party actors. Considering the sensitivity of the information Henry Ford possessed, Henry Ford was aware or should have been aware of the need to implement robust security measures to protect such information. It consciously refused to do so.

317. Accordingly, Plaintiff and each member of the Michigan subclass are entitled to, and seek, damages “for a violation of [the Reform Act] and may recover

actual damages or \$200.00, whichever is greater, together with reasonable attorneys' fees and costs.” § 550.1406(4).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class and appointing Plaintiff and Counsel to represent such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;
- D. For an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Nina McClain hereby demands that this matter be tried before a jury.

DATE: July 5, 2024

Respectfully submitted,

s/ Nicholas A. Coulson

Nicholas A. Coulson
Julia G. Haghighi
COULSON P.C.
300 River Place Drive
Detroit, MI 48207
T: (313) 644-2685
E: nick@coulsonpc.com
jprescott@coulsonpc.com

David S. Almeida*
Elena A. Belov*
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
T: (312) 576-3024
E: david@almeidalawgroup.com
E: elena@almeidalawgroup.com

Gary M. Klinger*
Glen L. Abramson*
Alexandra M. Honeycutt*
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com
gabramson@milberg.com
ahoneycutt@milberg.com

***Counsel for Plaintiff and the Putative
Classes***

** pro hac vice* forthcoming